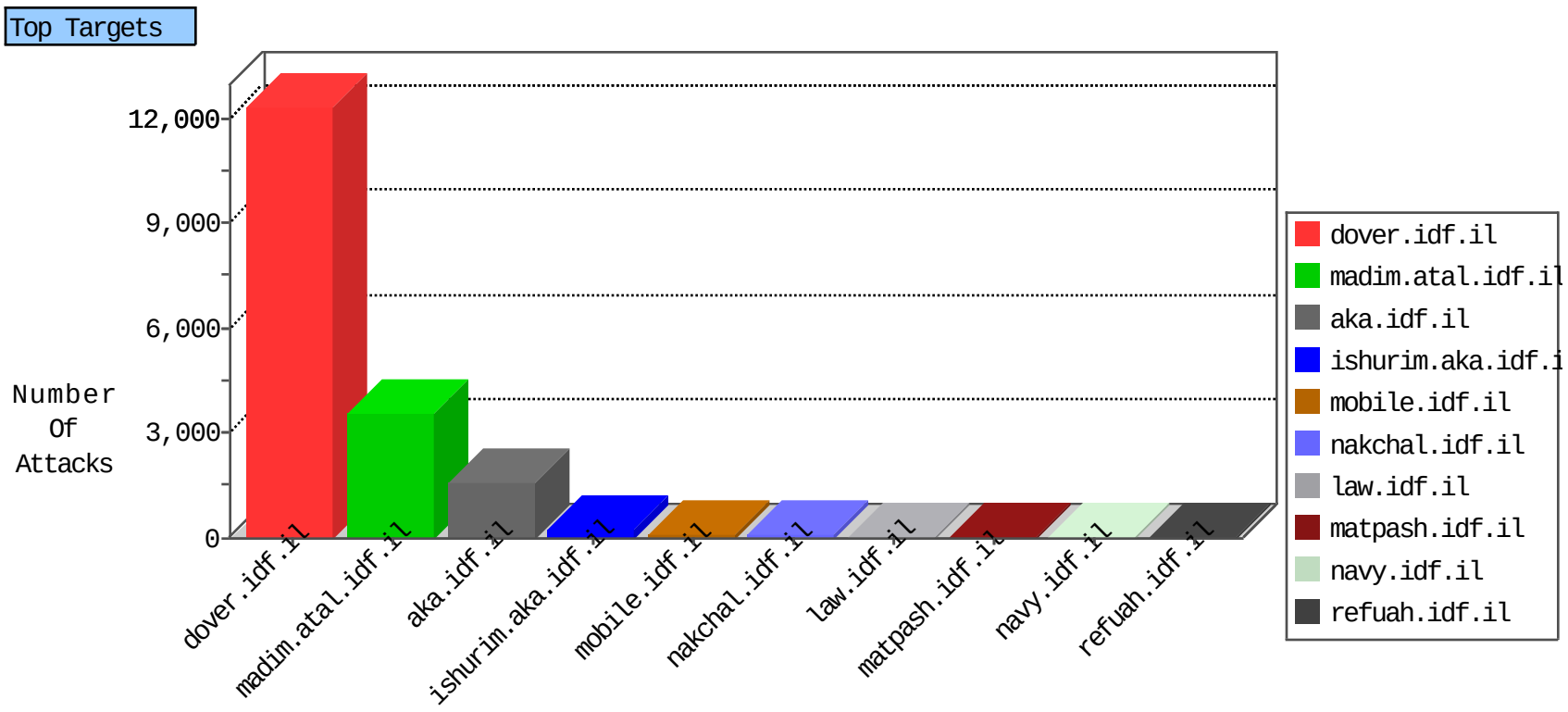
10-27-2015-10:04:00 to 10-27-2015-11:04:00

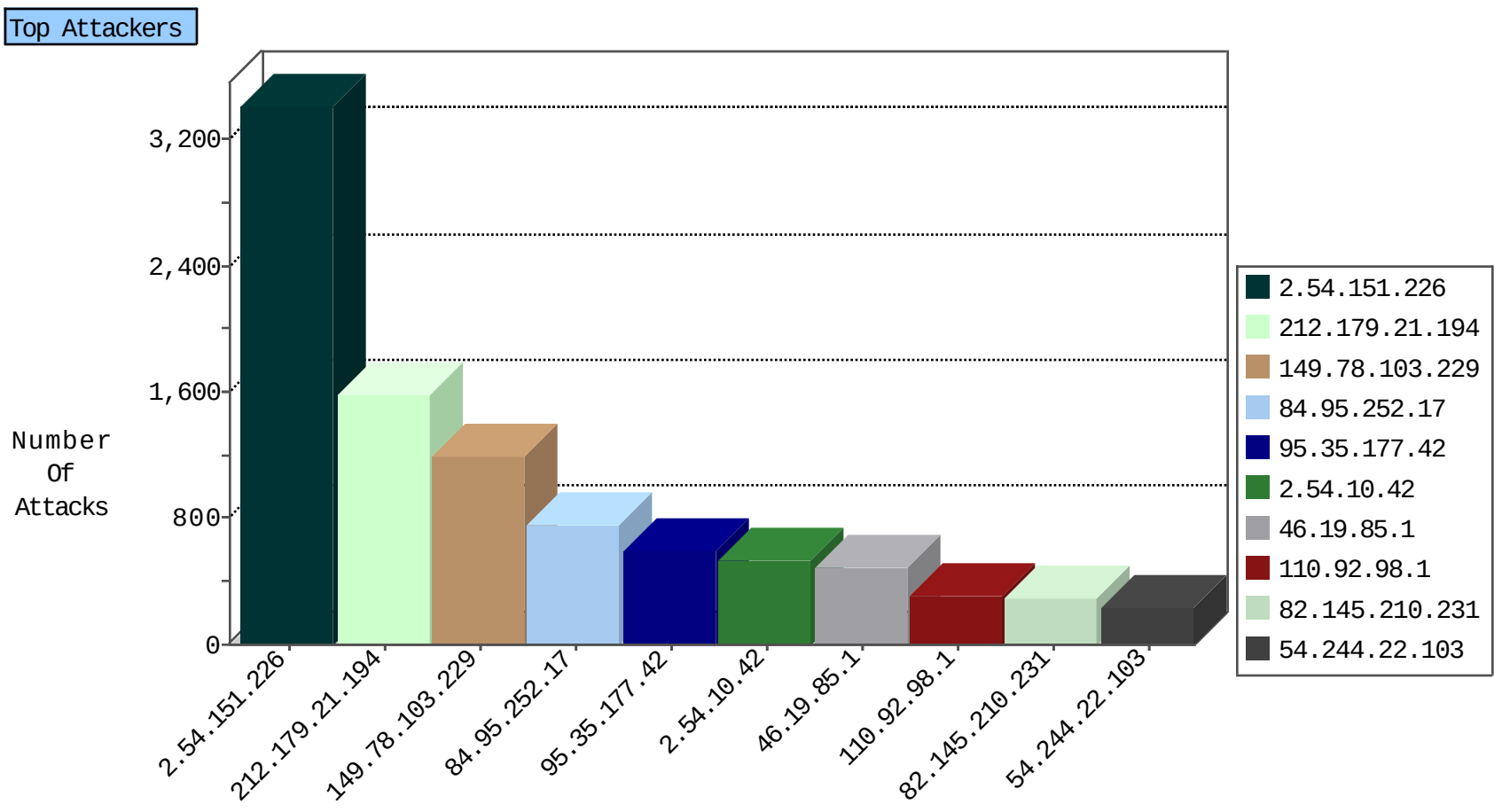
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-27-2015-10:04:00 to 10-27-2015-11:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.156.70.118	Turkey	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3372
46.19.86.109	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2751
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	188
66.249.67.227	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	70
46.19.85.212	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	41
46.120.78.148	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	20
192.114.87.2	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
132.72.79.166	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
212.143.3.44	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	11
2.54.12.29	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
109.67.59.17	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
80.246.136.56	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	8
109.64.205.148	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
2.52.39.185	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
192.114.105.254	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
95.35.177.42	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
79.179.37.115	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
80.179.82.129	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
62.219.128.153	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
109.67.116.108	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
37.26.147.233	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	5
46.19.86.215	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
220.148.25.197	Japan	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.178.36.143	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.12.150.212	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
85.112.78.242	Lebanon	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
192.114.1.131	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.52.39.185	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
194.90.66.15	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
37.26.146.214	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
2.54.45.175	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
79.183.51.228	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
109.67.116.108	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
193.203.232.5	Italy	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
217.132.94.28	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
82.145.210.231	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
217.194.203.76	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
194.114.146.227	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
185.32.179.36	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
149.78.154.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
89.100.238.100	Ireland	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
80.246.139.168	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
79.178.6.203	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
2.54.168.126	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
217.132.94.28	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.12.150.212	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
46.19.86.89	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
132.71.134.252	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
212.143.254.4	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2

10-27-2015-10:04:00 to 10-27-2015-11:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.117.219.208	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
62.90.255.56	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2

10-27-2015-10:04:00 to 10-27-2015-11:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.93.220	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
169.54.233.121	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
128.199.95.16	147.237.77.243	Singapore	mobile.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
91.216.51.37	147.237.77.216	Poland	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.106.67	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.151.52.8	147.237.72.14	Ukraine	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
37.142.216.243	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.45.253	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
169.54.233.121	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
122.176.253.254	147.237.77.216	India	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.118	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.209	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

10-27-2015-10:04:00 to 10-27-2015-11:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1575
149.78.103.229	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1193
84.95.252.17	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	765
95.35.177.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	585
2.54.10.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	529
110.92.98.1	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	301
82.145.210.231	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	287
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	223
194.25.30.10	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	216
195.160.240.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	187
31.168.87.76	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	159
141.0.15.170	Norway	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	147
193.203.232.5	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	130
212.156.70.118	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	122
91.228.167.130	Slovakia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	92
168.63.139.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	86
5.245.250.164	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	83
92.224.205.102	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	81
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	74
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
213.204.101.25	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
197.250.130.58	Tanzania, United Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
81.218.20.161	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
176.13.4.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
2.54.46.192	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
2.52.164.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
82.80.142.66	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
183.90.36.92	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
185.58.201.28	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
91.228.167.109	Slovakia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
109.64.133.137	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
41.218.184.118	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
62.219.130.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
212.179.28.34	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
220.148.25.197	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
209.133.111.215	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
31.210.186.143	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
212.106.72.118	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
31.186.228.31	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
31.186.228.59	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
176.13.4.126	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
109.65.24.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
31.186.228.29	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27

10-27-2015-10:04:00 to 10-27-2015-11:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.151.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3415
46.19.85.1	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.1	Block	490
46.19.85.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	154
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	56
217.194.207.24	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	42
95.86.95.69	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	42
213.151.56.234	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	42
176.12.137.157	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	28
109.66.164.194	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	28
2.54.13.50	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	28
176.12.151.30	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	28
109.66.164.194	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	28
109.67.177.241	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	28
46.117.219.208	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	28
2.52.29.196	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	28
109.67.177.241	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	28
149.78.49.220	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	28
188.143.232.21	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 188.143.232.21	Block	28
52.30.168.142	United States	147.237.77.235	sviva.idf.il	Unauthorized URL Access to 147.237.77.235/	Block	14
37.147.35.52	Russian Federation	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/9/	Block	14
79.183.113.124	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	14
188.143.232.21	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/1319-he/	Block	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	14
46.116.189.0	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/×?×™×©×•×¨×™×?	Block	14
128.199.95.16	Singapore	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/l12.tar	Block	14
31.44.138.99	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	14
79.177.123.95	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
212.199.185.108	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/mas.aspx	Block	14
54.215.187.95	United States	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	14
2.54.39.26	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
217.194.207.24	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	14
80.179.196.164	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	14
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	14
192.115.177.203	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mivtza	Block	14
46.117.219.208	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 46.117.219.208	Block	14
132.64.184.64	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	14
109.64.144.42	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
31.210.186.160	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	14
180.76.15.143	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	14
54.215.187.95	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	14
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	14
66.249.93.199	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/homas/site/	Block	14
141.212.122.160	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	14
109.64.205.148	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	14
37.26.149.181	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
213.151.57.14	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	14
79.182.206.205	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.182.206.205	Block	14
185.32.179.132	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
66.249.67.219	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/civiladministration/govermment/_layouts/authenticate.aspx	Block	14

10-27-2015-10:04:00 to 10-27-2015-11:04:00